



1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings of a security assessment conducted on the domain `familycu-dc.cert.fec-d`. The analysis was performed using a Basic scan type, initiated on **May 26th** at **02:45** and completed in **00h:09m:40s**. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, following OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** high-risk, **1** medium-risk, **1** low-risk, and **16** informational. The most significant finding is a medium-risk issue related to an open HTTP port (**80**) that lacks encryption, potentially exposing sensitive data if not redirected to HTTPS. This vulnerability could lead to data breaches if exploited. Additionally, the SSL/TLS protocol analysis revealed that all endpoints support modern TLS **1.2** and **1.3**, ensuring strong encryption standards. No shared hosting environments or brute-force susceptible services were detected, indicating a robust infrastructure. It is recommended to address the HTTP port issue promptly to mitigate potential security risks.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Nmap Port Scan Results Analysis

Description

The assessment identified an open HTTP port (**80**) running the `volt-adc` service without encryption. This poses a risk of data exposure if not properly redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled. A total of **2** open ports were detected during the scan.

Affected Assets

- IP: **107.162.254.128**
- Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations

Immediate action should be taken to ensure that all HTTP traffic is redirected to HTTPS. Implementing HSTS can further enhance security by preventing protocol downgrade attacks and cookie hijacking.

1.3.2 SSL/TLS Protocols Security Assessment

Description

The SSL/TLS protocol analysis confirmed that all endpoints support modern encryption standards, with one endpoint using TLS **1.3** and another using TLS **1.2**. No endpoints were found using deprecated protocols such as SSLv3, TLS **1.0**, or TLS **1.1**, which are vulnerable to known attacks like POODLE and BEAST.

Affected Assets



- 1 endpoint with modern TLS 1.3 support.
- 1 endpoint using TLS 1.2.

Recommendations

Continue to maintain and monitor the use of TLS 1.2 and TLS 1.3 across all endpoints to ensure compliance with current best practices in encryption standards.

1.4 General Recommendation

To enhance the overall security posture, it is recommended to regularly review and update security configurations, ensuring that all services are running on secure protocols and that any deprecated or insecure services are promptly addressed. Regular security assessments should be conducted to identify and mitigate potential vulnerabilities proactively.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING